EXHIBIT 5

Data processing by the employer

What are the requirements that employers must meet when processing personal data?

Frequently asked questions (selected examples)

Legal basis

Code of Obligations of 30 March 1911 (CO)
Recruitment Act (available in German, French and Italian)

Recruitment Ordinance (available in German, French and Italian)

Different phases of the employment relationship

(/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenbearbeitung-arbeitgeber/datenbearbeitung_arbeitgeber_phasen.html)

What data are employers allowed to use? What do they have to do?

In employment relationships governed by private law, the employer is required to process a large amount of personal data of his employees, including sensitive data and employee profiles during the various stages of the employer-employee relationship. However, the employer must protect and respect the personality rights of his employees.

While the employer is primarily responsible for data protection in the workplace, employees or future employees can also ensure that their data is processed properly and deleted within the prescribed period. Data processing must be carried out within reasonable limits and be proportionate to the purpose. Since the relationship of trust between employer and employee determines the quality of the work done in the company, it is essential that the employer always informs employees precisely of their rights and of the data processing carried out.

In accordance with Article 328 paragraph 1 of the Swiss Code of Obligations (CO), within the employment relationship, the employer must acknowledge and safeguard the employee's personality rights. This provision entails a general duty of assistance on the part of the employer towards its employees, an obligation which is the counterpart of the duty of loyalty assigned to the employee in Article 321a CO. The employer must avoid any infringement of the employee's personality rights that is not justified by the employment contract. Article 328b CO complements the Data Protection Act (FADP) in that it determines the nature of the information that the employer is entitled to process about its employees. In accordance with Article 328b, an employer may handle data concerning an employee only to the extent that such data concern the employee’s suitability for the job or are necessary for the performance of the employment contract. This article, which applies specifically to employment contracts, specifies the general principles of data processing, including the principle of proportionality. Under no circumstances may Article 328b CO be derogated from to the detriment of the employee, even if the latter consents (Art. 362 CO).

Outside the framework of Article 328b CO, the processing of data by the employer must be justified for other reasons (such as the consent of the employee, by an overriding private or public interest, or by law, see Art. 31 FADP. However, employees are very rarely in a position to freely give, refuse or revoke their consent, given the subordinate nature of the employer/employee relationship). Employers must also comply with the general principles of data protection so as not to violate the personality rights of their employees (Art. 30 FADP) and expose themselves to legal action (Art. 32 FADP) or, in certain circumstances, to an

investigation by the FDPIC (Art. 49 FADP), not to mention other legal remedies provided for in specific legislation (Art. 179ss Criminal Code, Art. 59 EmpA). The court decides in the individual case whether or not the data processing is justified.

Otherwise, the provisions of the Data Protection Act (FADP) apply. The processing of data by private employers is governed mainly by the general principles defined in this area (Art. 6 to 8 FADP), by the provisions on the right to information (Art. 25 and 26 FADP) and by the provisions on the processing of personal data by private persons (Art. 30 et seq. FADP).

The FADP also imposes other obligations on employers in certain circumstances (e.g. Art. 12 FADP: obligation to maintain an inventory of processing activities; Art. 14: obligation to appoint a representative in Switzerland when the private controller has its registered office or domicile abroad; Art. 19 to 21: Duty to provide information when collecting personal data and in the case of automated individual decisions; Art. 22: obligation to carry out a personal data protection impact assessment where the processing operation is likely to result in a high risk to the personality or fundamental rights of the person whose data is processed (the data subject); Art. 24: obligation to report data security breaches).

Employment agencies and service providers are subject to the requirements of the Recruitment Act (RecA) and the related ordinance (RecO), in particular Articles 19 and 47 RecO.

Frequently asked questions (selected examples)

Transferring personal data abroad

Many employers decide to have their employees' personal data processed abroad to save on costs or for organisational reasons. Data are considered to have been transferred abroad when they have been made accessible to a company or unit based abroad or when they are hosted in a cloud located abroad. According to the FDPIC, employers are responsible for ensuring that the transfer of personal data abroad is permitted . They must also provide full internal information on the transfer of data abroad as well as on the specific data processing carried out abroad and its purposes. This information includes which country the data is exported to and which companies it is transmitted to, as well as the evaluations that are carried out and the purpose behind them. A civil court may be required to decide in specific cases whether the transfer of data is lawful and whether appropriate information has been provided to the people whose data is being processed (data subjects).

cross-border transfer of personal data

(/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html)

Health issues

When recruiting employees, employers are only permitted to ask about the applicant's qualifications or other significant facts relevant to how well they can perform the tasks set out in the employment contract. Employers are not allowed to enquire about an applicant's general health; however, they can ask for a medical report on the applicant's fitness for the job in question. Prior illnesses, surgeries and hospital stays are only relevant in this context if they would have an impact on the applicant's suitability for the position being filled.

The same applies to any benefits or pensions that the applicant has received due to illness, provided that the associated illness does not affect the applicant's ability to perform their new job. The employer can require a medical examination under certain circumstances, for example in occupations where health problems may present significant safety or other risks. In such cases, the doctor is responsible for determining whether the applicant's current or prior illnesses, including any treatments they are currently receiving or have received in the past, are compatible with the job they are applying for. The doctor performing the medical examination is bound by doctor–patient confidentiality. This means that they are only allowed to inform the employer of results that are relevant to the candidate's suitability for the position being filled. They cannot disclose any other information about the candidate's medical history. This rule also applies when the medical examination is carried out by the company's in-house doctor. The doctor's opinion on fitness for work, including any reservations they may have, is then given to the employer for inclusion in the employee's personal file. The medical file, however, remains with the doctor.

Using fingerprints to monitor access and working time

Biometric systems to record working time and to control system access are becoming increasingly common in some sectors. Sensitive data such as fingerprints should only be used after careful consideration and in an appropriately restricted fashion. Some widely used biometric systems that record working time, control system access and manage tills require employees to identify themselves using their fingerprints. Employees are sometimes required to consent to their fingerprints being recorded in order to conclude or continue an employment contract. Fingerprints and other biometric data are inherently tied to a person and cannot simply be changed if lost. Heightened security requirements therefore apply to the processing of these sensitive personal data. In particular, they may only be processed if the processing is necessary for the intended purpose. In order to prevent unauthorised third-party access to employees' biometric data, the data must not be stored centrally on a server. Instead, it should only be stored on a local medium, e.g. a badge, which must be read at the same time as the fingerprints. It is recommended that only a single fingerprint be processed (rather than the complete set of fingerprints) in line with the principle of proportionality. It would be advisable to offer employees alternatives to biometric methods of recording working time, in order to preserve their freedom of choice. It is primarily a matter of employment law whether an employer is allowed to require an employee to provide fingerprints in order to be hired. Individual employees can go to court to challenge the introduction of biometric time recording systems.

Remote working

Employment law defines the conditions that allow for employees to work remotely. Remote working nevertheless raises a number of important issues relating to data protection, for example regarding the use of digital communication technologies for conference calls and videoconferencing, as well as the use of data exchange platforms. Employee obligations may change occasionally, but the employer remains responsible for information security and data protection, even in times of crisis, and is therefore bound by the data processing principles set out in the FADP. This includes the obligation to choose software that adequately guarantees the security of the personal data being processed. The Commissioner is aware that there are IT solutions that enable employers to constantly monitor the behaviour of employees who are working remotely. However, this is generally not permitted under the FADP and furthermore is expressly forbidden under employment law. Finally, the question arises as to whether there is disclosure of data abroad if the employee is working remotely from outside of the country and accesses the company's server in Switzerland from their location abroad, for example in holiday accommodation or, in the case of cross-border commuters, at home. This does not constitute transborder data disclosure within the meaning of the FADP as long as the employee uses a virtual private network (VPN) to access the company's server while abroad, processes the personal data only to the extent that they would normally do so in the company's offices and, most importantly, does not make the data accessible to anyone abroad. The confidentiality of personal data must always be guaranteed, whether employees are working remotely from abroad or in Switzerland.

Extracts from the debt enforcement register and the criminal records register

In line with the data protection principles, employers can request extracts from the debt enforcement register and the criminal records register only if the employee will be working in a position of trust, or carrying out duties such as managing customer accounts or operating tills or safes. This includes roles in which employees are in contact with or responsible for valuable goods or large sums of money. In these cases, the security of the company takes precedence over the interest in protecting privacy.There is no legitimate interest worthy of protection that would justify a systematic review of an employee’s credit rating or whether they have a criminal record.

If extracts from the debt enforcement or criminal records registers contain sensitive data, the data protection principles must be followed strictly. Employers must provide the person concerned with clear and complete information about the data that has been collected and grant them the right to access the data. There must be effective protection from unauthorised data access, the number of parties given authorised access must be restricted as much as possible, and the data must be destroyed as soon as it is no longer required.

Publishing photos of employees on the intranet or internet

Publishing photos of employees on the company's intranet or on the internet requires the consent of the persons concerned, as a photograph can in some cases be used to determine information about the subject, such as a person’s religion or race, or whether they have a

physical impairment. Often the publication of photographs serves no practical purpose, especially photos taken at events organised by the employer such as drinks receptions and excursions. It is advisable to first consider whether there is any benefit in publishing employee photos.

Using artificial intelligence in recruitment

Recruitment processes increasingly involve artificial intelligence. For example, artificial intelligence helps to select applications, while job interviews are recorded on video and then analysed by software. Similarly, in today's workplace automated behaviour and voice analyses are increasingly used in online application processes to draw up detailed profiles. This requires a higher level of data protection. Candidates and recruiters alike have questions about the permitted use of behaviour and voice analysis and the associated legal requirements. The data protection framework that applies to traditional recruitment procedures also applies to these new instruments. Employers may only collect and process the data that is necessary to determine a person's suitability for a particular job, and they must always respect the principles set out in the legislation on data protection. In addition, the vast possibilities of AI-based analyses generally allow for more serious violations of personality rights than conventional job interviews. The principles of recognisability and proportionality must be given particular attention in this context.

Access to employees' emails (/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenbearbeitung-arbeitgeber/zugriff_mail.html)

The question of when employers can have access to employees' emails raises a number of issues for both employees and employers. It is not always easy to draw a line between the legitimate interests of employers and the privacy of their employees.

Recording conversations (/edoeb/en/home/datenschutz/arbeit_wirtschaft/audioueberwachung.html)

Anyone who unlawfully records a conversation may be in violation of the Data Protection Act (DPA), not to mention the Criminal Code (SCC).

Video surveillance in the workplace (/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenbearbeitung-arbeitgeber/videoueberwachung-arbeitsplatz.html)

Video surveillance systems can affect the well-being, mental health and productivity of employees, and should therefore only be considered when less invasive measures are genuinely unsuitable.

Telephone monitoring in the workplace
(/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenbearbeitung-arbeitgeber/ueberwachung_arbeit.html)

There are many questions about telephone monitoring in the workplace, and in particular when monitoring is allowed.

 (/edoeb/en/home/deredoeb/kontakt/faq_beratung1.html)

Questions on data protection (/edoeb/en/home/deredoeb/kontakt/faq_beratung1.html)

Take a look at our FAQ or call our hotline.

 (/edoeb/en/home/datenschutz/grundlagen/ndsg.html)

The main provisions (/edoeb/en/home/datenschutz/grundlagen/ndsg.html)

Here you can find out more about changes to the Data Protection Act, which came into force on 1 September 2023.

 (/edoeb/en/home/deredoeb/kontakt.html)

Contact (/edoeb/en/home/deredoeb/kontakt.html)

 (/edoeb/en/home/deredoeb/infothek.html)

Infocenter (/edoeb/en/home/deredoeb/infothek.html)

Here you can download all documents sorted by topics.

Webmaster (mailto:webmaster@edoeb.admin.ch)

Last modification 25.06.2024